## 1NC — China Relations

### 1NC — China Relations Frontline

#### 1. The plan has a low risk of solvency and massive timeframe for action.

Nathan 12 — Andrew Nathan, Professor of Political Science at Columbia University, Chair of the Steering Committee for the Center for the Study of Human Rights, Ph.D. in Political Science from Harvard University, M.A. in East Asian Studies from Harvard University, 2012 (“Cybersecurity and U.S.-China Relations,” *Foreign Affairs,* September/October, Accessible Online at <https://www.foreignaffairs.com/reviews/capsule-review/cybersecurity-and-us-china-relations>, Accessed On 06-28-2016, MA)

\*This is a review of the Leiberthal and Singer Evidence.

This report considers how hacking, cyber-espionage, and the threat of cyberwarfare affect U.S.-Chinese relations. Americans hear more about Chinese threats to the United States than vice versa, but it is likely that U.S. private and government actors are probing China’s Internet as much or more than the Chinese are probing that of the United States. And in cyberspace, the advantage goes to the offense. On key issues relating to the Internet, Chinese and U.S. interests are fundamentally opposed. The United States favors information freedom, whereas China’s regime relies on control. The U.S. military operates on cybernetworks, whereas the Chinese quest for asymmetric strategies requires the capability to take such networks down. Even dialogue, which Lieberthal and Singer advocate as a first step in a long march, will be a challenge, given the diffusion of control over the Internet within each society. Moreover, one wonders whether even two such important powers can do much to enhance cyber-security when potential attackers are globally dispersed and often private.

#### 2. US-Sino relations high now – military-to-military stabilization

Stratfor 15 — Stratfor, global awareness forecasters who analyze world affairs, 2015 (A New High for U.S.-China Military Ties,” *Stratfor*, December 4, 2015, Available Online at <https://www.stratfor.com/analysis/new-high-us-china-military-ties>, Accessed June 30, 2016//AW)

In recent years, the military-to-military relationship has begun to stabilize once again. Although it is by no means back to pre-1989 levels, neither country has canceled major military interactions since 2011. This improvement roughly corresponds with the start of Xi Jinping's tenure as vice chairman of China's Central Military Commission, the military's core leadership body, in October 2010. He later became chairman in November 2012. This was an early indication of his interest in strengthening military-to-military relations during his presidency, which began in March 2013. Under Xi, the People's Liberation Army has increased the frequency of joint drills with the U.S. military, culminating in the United States inviting the Chinese navy to participate in RIMPAC 2014, the world's largest multilateral naval exercise. This was a symbolic milestone. The People's Liberation Army also built up its regularized communication mechanisms with the U.S. military, including the army-to-army dialogue that kicked off in November. More critically, the Chinese military made a serious effort to establish and implement crisis management mechanisms. At the 2014 Western Pacific Naval Symposium, the People's Liberation Army Navy agreed to abide by the Code for Unplanned Encounters at Sea, which establishes common protocols for interactions between naval vessels to reduce accidents. In September, China signed a bilateral agreement with the United States governing air-to-air encounters as well as protocols governing the use of the Defense Telephone Link. The two navies are also set to hammer out a set of rules on ship-to-ship encounters in the near future.

#### 3. Alt Causes to Relations:

#### A. Territorial Disputes — land reclamation in the South China sea threatens Freedom of Navigation

Johnson 15 — William Johnson, retired US Air Force Officer and retired Foreign Service Officer, 2015 (“The five most important issues in U.S.-China relations,” *Reuters*, June 23, 2015, Available Online at <http://blogs.reuters.com/great-debate/2015/06/23/the-five-most-important-issues-in-u-s-china-relations/>, Accessed June 30, 2016//AW)

This year’s dialogue has special significance because it will set the stage for President Xi’s state visit in September. U.S.-China relations have been rocky recently, owing primarily to tensions in the South China Sea, China’s new law governing foreign non-governmental organizations, and friction over membership in China’s Asian Infrastructure Investment Bank and the U.S.-led Trans-Pacific Partnership (TPP). In addition to these issues, Chinese and American leaders will devote substantial attention to cybersecurity and the recently disclosed hack of the Office of Personnel Management’s database, as well as the ongoing negotiations toward a U.S.-China Bilateral Investment Treaty (BIT). The diplomatic community has expected previous dialogues to produce substantial agreements, but they have lower expectations for this round — due partly to recent difficulties in the relationship, as well as an inclination on both sides to save major announcements until President Xi’s state visit. I’ll briefly explain the significance of these five major issues. 1. The South China Sea The South China Sea issue has been front and center for the last 18 months, as China carried out major land reclamation efforts. While the issue stems from territorial disputes between China and various Southeast Asian nations, which don’t intrinsically involve the United States, the United States sees China’s island building activities as a potential threat to freedom of navigation along a critical trade route. China, on the other hand, sees U.S. involvement in the region as meddling in bilateral disputes with China’s neighbors. It sees enhanced U.S. military cooperation with Vietnam and the Philippines, and increased Japanese military activity in the region, as part of a U.S. strategy to contain China. The 2015 dialogue provides an opportunity to ratchet down the recent level of confrontation in order to smooth the way to a successful state visit by President Xi.

#### B. Human Rights — Chinese censorship fosters mistrust and misunderstanding

Cook 15 — Sarah Cook, senior research analyst for East Asia at Freedom House, B.A. in International Relations from Pomona College, Masters in Politics and International Law at the School of Oriental and African Studies in London as a Marshall Scholar, 2015 ("How Beijing’s Censorship Impairs U.S.-China Relations," *Freedom House*, July 23rd, Available Online at https://freedomhouse.org/blog/how-beijing-s-censorship-impairs-us-china-relations, Accessed 6-30-2016//AW)

Over time, the various obstacles thrown up by Beijing have had a deleterious effect on international news coverage and information sharing on important topics. But even as foreigners feel the impact, it remains Chinese citizens who pay most dearly for their government’s censorship. The Communist Party’s latest blocks and regulations have increased the share of the Chinese population that is losing contact with the international community and its diverse information sources. According to one college counselor from Shanghai, the censorship adds new difficulties for Chinese students applying to study at U.S. universities and, more generally, limits their worldview. Consequences for U.S.-China relations From a geopolitical perspective, these developments have a profound impact on the relationship between the world’s two largest economies. The divided and distorted information landscape breeds mistrust and increases the potential for misunderstanding. Chinese audiences receive a partial and misinformed perspective of U.S. policy and society. Americans see Chinese officials taking steps that threaten the United States’ economic wellbeing, but are barred from hearing the views of Chinese citizens who may disagree with their government. This results in both sides having a more negative view of the other than each may deserve, a recipe for greater tension now and in the future. On a more practical note, the restrictions create higher hurdles for U.S. investment in China and hinder day-to-day cooperation in the arts, non-profit, and academic sectors. Moreover, the Chinese government’s actions contradict its own stated policies, like not interfering in other countries’ affairs, and undermine key goals popular with China’s citizens, such as earning global respect for the nation.

#### C. Economics — the AIIB and TPP are thorns in the relationship

Johnson 15 — William Johnson, retired US Air Force Officer and retired Foreign Service Officer, 2015 (“The five most important issues in U.S.-China relations,” *Reuters*, June 23rd, Available Online at <http://blogs.reuters.com/great-debate/2015/06/23/the-five-most-important-issues-in-u-s-china-relations/>, Accessed June 30, 2016//AW)

3. Friction Over Membership in China’s Asian Infrastructure Investment Bank Economic alignments in East Asia will likely be a central focus of this year’s dialogue. China is in the process of starting the Asian Infrastructure Investment Bank, which is intended to provide more streamlined funding than the World Bank or the Asian Development Bank can currently provide. The United States opposed the establishment of the AIIB — and lobbied its allies to decline membership — on the grounds that it had unclear governance standards, inadequate environmental controls, and might not be sufficiently capitalized to sustain its loans. But in the week before a March deadline, the United States suffered a stinging defeat as its allies, led by the United Kingdom, became founding members of the bank, leaving the United States and Japan on the outside looking in. Governance of the AIIB, and a means for coordinating its efforts with the World Bank, will be key elements of the economic discussions. In a similar vein, the U.S.-led TPP includes the United States and Japan as the key members of what would be the largest trade agreement ever. The difference here is that China is the outsider. China has complained that the TPP is yet another instance of the United States trying to contain China. President Obama’s recent remark that the U.S. must write the rules for trade, or China will, didn’t dispel this notion.

### Extend: “Alt Causes to Relations”

#### Non-cyber issues subsume and strain the US China relationship:

#### - China’s land reclamation efforts in the South China Sea threaten Freedom of Navigation on a critical trade route

#### - The Great Firewall along with the American public’s anti-Chinese sentiment foments mistrust between societies

#### - US opposition to the Asian Infrastructure Investment Bank and Chinese opposition to the Trans-Pacific Partnership strain the economic relationship as exclusionary international agreements

#### The burden of territorial, economic, and human rights disputes make broader Chinese cooperation extremely difficult even if cooperation exists on cybersecurity — that’s Johnson and Cook.

#### And, human rights pressure on NGO laws places pressure on the relationship

Johnson 15 — William Johnson, retired US Air Force Officer and retired Foreign Service Officer, 2015 (“The five most important issues in U.S.-China relations,” *Reuters*, June 23rd, Available Online at <http://blogs.reuters.com/great-debate/2015/06/23/the-five-most-important-issues-in-u-s-china-relations/>, Accessed June 30, 2016//AW)

2. China’s New Law Governing Foreign NGOs China’s new draft law on NGOs will substantially limit the ability of a wide range of organizations to work in China. The key sticking point in the new law is that it places regulatory authority over foreign NGOs with China’s State Security Bureau, rather than the Ministry of Civil Affairs, which regulates domestic NGOs. Police will be allowed to enter and inspect offices, and seize documents and equipment. The United States has long been critical of China’s record on human rights, and this proposed law, which was released for comment on June 8, will be a focal point in that discussion. China’s response to U.S. pressure on this issue will likely turn on its view that foreign elements are stirring up trouble in China. This is the same argument that China used to explain the Occupy Central pro-democracy demonstrations in Hong Kong. Reading between the lines, it is clear that in both instances, when China says “foreign elements,” it means the United States and its allies.

## 1NC — Cybersecurity

### 1NC — Cybersecurity Frontline

#### 1. US-China cyber-cooperation doesn’t solve cyberattacks — no enforcement.

Tiezzi 15 — Shannon Tiezzi, Editor at The Diplomat, Research Associate at the US-China Policy Foundation, A.M. in Asia Studies from Harvard University, 2015 (“The Limits of a US-China Cyber Deal,” *The Diplomat,* September 22nd, Accessible Online at <http://thediplomat.com/2015/09/the-limits-of-a-us-china-cyber-deal/>, Accessed On 06-28-2016, MA)

Unless a U.S.-China agreement goes far beyond the GGE report (and, on the contrary, Sanger expects an endorsement of the UN document), this vagueness will limit its actual utility in the real world. As Grigsby points out, it’s not too far of a stretch to argue that the November 2014 hack against Sony Pictures could be an attack on “critical infrastructure” according to the U.S. definition.

And then there is the question of enforcement – what sort of response would a violation of the deal (particularly a low-level one, such as the Sony hack) elicit? That issue is particularly complicated given the problem of attribution when it comes to cyber attacks, and the potential for non-state actors to launch attacks. China, for one, frequently points out that simply because an attack was carried out on its soil doesn’t mean the government had any involvement.

Even if the deal is concluded and improves upon the GGE report by clarifying these essential questions (unlikely), it still wouldn’t address a fundamental disagreement on the limits of cyber espionage. Cyber attacks for financial gain – aimed at stealing intellectual property, business strategies, and other proprietary information – are a separate issue from the use of offensive-minded cyber attacks designed to shut down real-world targets. The agreement, as reported on by Sanger, would deal exclusively with the latter even though economic cyber espionage has been the main issue for the U.S.-China relationship.

#### 2. Alt Cause to Cybernorms — US Cyber-Hypocrisy.

Gady 16 — Franz-Stefan Gady, Senior Fellow and Foreign Policy Analyst at the East-West Institute, Editor at *The Diplomat,* M.A. in International Relations from John Hopkins University, B.A. in International Relations from Weber University, 2016 (“Are Chinese Cyberattacks Against US Targets in Decline?,” *The Diplomat,* July 23rd, Accessed Online at 6-28-2016, MA)

However, ever since the Snowden revelations, the United States found it difficult to advance this unwritten norm as a new modus vivendi in dealing with adversaries in cyberspace. The Chinese in particular accused the United States’ government to apply double standards after some previously unknown U.S. cyberespionage activities were made public.

For example, evidence emerged back in April 2015 that the United States has been engaged in some form of economic espionage in Europe. One analyst, writing for the Washington Post, notes that this new incident “will be moderately embarrassing for the United States, which is currently trying to build international norms against economic espionage.”

He continues:

It isn’t at all clear that the United States was committing economic espionage by its own definition (it argues that it can legitimately conduct espionage against economic targets such as businesses as long as it is for strategic purposes, and the information is not passed along to U.S. firms). However, it certainly greatly complicates the story that the United States is trying to tell.

Consequently, we can assume that the Obama administration’s reluctance to “name and shame” China as a culprit in the OPM hack is partially connected to the Snowden leaks and the loss of U.S. legitimacy as a fair arbiter of norms.

#### 3. No Impact Uniqueness — Chinese cyberattacks are declining.

Gady 16 — Franz-Stefan Gady, Senior Fellow and Foreign Policy Analyst at the East-West Institute, Editor at *The Diplomat,* M.A. in International Relations from John Hopkins University, B.A. in International Relations from Weber University, 2016 (“Are Chinese Cyberattacks Against US Targets in Decline?,” *The Diplomat,* June 22nd, Accessed Online at 6-28-2016, MA)

A new report argues that there has been a decline in the number of Chinese cyberattacks against U.S. targets.

Since the middle of 2014, cyberattacks by China-based hacking groups against the U.S. government and private sector have declined, according to a June 2016 analysis by the U.S. cybersecurity firm FireEye.

A FireEye team reviewed the activities of 72 hacking groups purportedly operating out of China or supporting Chinese state interests from the beginning of 2013 to June 2016.

“Since mid-2014, we have observed an overall decrease in successful network compromises by China-based groups against organizations in the U.S. and 25 other countries,” the report notes.

#### 4. Norms don’t prevent cyber proliferation — no concrete assurances and not everyone is convinced.

Stevens 12 — Tim Stevens, Professor of Politics at King’s College London, 2012 (“A Cyberwar of Ideas? Deterrence and Norms in Cyberspace,” *Contemporary Security Policy,* Vol. 33, No. 1, Accessible Online via SSRN at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764>, Accessed On 06-28-2016, MA)

Yet the question remains: how effective is a norms-based approach to cyber deterrence likely to be? How can we tell what aspects of a deterrence strategy are working, or which aren’t? In truth, it is much too early to know. Even if it were possible to get all parties to comply with a set of norms hammered out through diplomacy and other forms of negotiation, what guarantees are there that these would be adhered to? Again, there are no such guarantees. It may be that states can be persuaded to comply with international normative frameworks through a mix of inducement, coercion and moral pressure. So too might industry and civil society be persuaded to do their part through a gradual process of cultural learning, and all parties work together to achieve the ‘global culture of cybersecurity’ currently aspired to. Even were these norms to operate strongly and bind together these actors such that norms of non-use or acceptable use became institutionalised, they are never likely to persuade all who might have the capabilities to prosecute actions in cyberspace that constitute strategic threats. For this reason alone, states and their militaries and security services will, even whilst pursuing denial strategies and improving defensive cybersecurity, be loath to abandon the search for effective punitive measures through which deterrence might be achieved. In turn, the norm of retaliatory punishment may prove to be a powerful deterrent in itself.

#### 5. Timeframe is massive — norms take decades to develop.

Nye 15 — Joseph Nye, University Professor at Harvard University, former US assistant secretary of defense and chairman of the US National Intelligence Council (“International Norms in Cyberspace,” *Project Syndicate,* May 11th, Accessible Online at <http://www.project-syndicate.org/commentary/international-norms-cyberspace-by-joseph-s--nye-2015-05#w8h0eeipk0PGeqL2.99>, Accessed 06-28-2016, MA)

Nonetheless, some institutions, both formal and informal, already govern the basic functioning of the Internet.

The US wisely plans to strengthen the non-governmental Internet Corporation for Assigned Names and Numbers (ICANN) by having it supervise the Internet “address book”.

And a UN Group of Governmental Experts has been analysing how international law relates to cybersecurity.

It is likely to take longer to conclude agreements on contentious issues such as cyberintrusions for purposes such as espionage and preparing the battlefield.

Nonetheless, the inability to envisage an overall cyberarms-control agreement need not prevent progress on some issues now. International norms tend to develop slowly. It took two decades in the case of nuclear technology.

The most important message of the recent Dutch conference was that massive cybervulnerability is now nearing that point.

#### 6. Their evidence is biased to over-hype the Chinese cyberthreat.

Austin 15 — Greg Austin, Professorial Fellow at the East-West Institute, Professor at the Australian Center for Cybersecurity, 2015 (“Cyber Security: All China’s Fault?,” *The Globalist,* August 30th, Accessible Online at <http://www.theglobalist.com/cyber-diplomacy-us-china-problem/>, Accessed On 06-29-2016, MA)

Then there is the eternal Washington “logic” of bureaucratic politics. Consider this. On the one hand, security chiefs all across the United States already have staggeringly large budgets and resources at their disposal.

On the other hand, it is very difficult for them to admit that their technical skills and technologies have not been good enough in most cases to stop China’s cyber thievery.

Would it be surprising therefore for all of them to fall unconsciously into finding a common public scapegoat, a “whipping boy,” a strategy that downplays other bad cyber actors, such as Russia, Israel, France and even Iran? Enter the China blame game.

This is not to say by any means that China is without fault. Far from it. But what is equally undeniable is that the impact of the China cyber threat relative to other threats is exaggerated by the U.S. cybersecurity community.

The other side of that same coin is that the U.S. capabilities and reach into Chinese networks is conveniently belittled – and strategically obscured.

Major U.S. media, always interested in their ratings and click statistics, are all too happy propagators of that one-sided threat world.

#### 7. No Risk of US-China Cyberwar — deterrence.

Roberts 12 — Paul Roberts, Founder of the Security Ledger and Security of Things Forum, a website and forum for discussion, Editor at ThreatPost, a newswire of Kapersky Lab, a cybersecurity firm, 2012 (“Despite Intrusions, Chances of U.S.-China Cyber War Are Small,” *ThreatPost,* March 1st, Accessible Online at <https://threatpost.com/despite-intrusions-chances-us-china-cyber-war-are-small-030112/76271/>, Accessed On 06-30-2016)

A panel of security and policy experts said that, despite dire warnings about the information warfare capabilities of China and other developing nations, the risk of an all-out cyber war is remote, and that the U.S. still holds many of the cards.

Despite widespread portrayals of China as a cyber aggressor, the country’s civilian and military leaders are seeking input from U.S. policy experts as they weigh the role that cyber offense and defense will play in their country’s foreign policy and defense, the panel told attendees at the RSA Security Conference in San Francisco on Wednesday.

The cadre of top cyber security policy experts took part in a panel titled Cyber Battlefield: The Future of Conflict on Wednesday. Panel members offered differing opinions about the dimensions of the cyber threat, but a consensus on the need for using tried and true methods in the new realm of cyber conflict. International diplomacy, multilateral agreements that clarify the parameters for peaceful and hostile cyber actions and a strong offensive deterrent were a must, experts said.

“With China, multilateral efforts are particularly important,” said Adam Segal, A Senior Fellow for Counter Terrorism and National Security Studies at the Council on Foreign Relations. “If we can get India, Brazil, South Africa and other countries join with us, we’ll have a lot better chance of getting the Chinese to see things our way.”

Old fashioned diplomatic horse trading will also be a critical tool for avoiding conflict and stemming the kinds of economic and military espionage that have become common in recent years.

“We have our list of priorities and the Chinese have theirs,” said Dmitri Alperovitch of the firm CrowdStrike. “There has to be some sort of diplomatic transfer where we there’s a trade off.”

The U.S. also has to start building up its allies by sharing its native cybersecurity expertise.

“There’s a huge need for capacity building in these countries where the security expertise is thin on the ground,” Segal said. “If we’re not in there, then (Mainland networking technology firm) Huawei and the Chinese will be, and you’ll end up with different norms about information flow and control.”

Finally, deterrence will play an important role in avoiding conflict, as it did in the Cold War with Russia.

The Chinese military appreciates that both it and the U.S. have cyber offensive capabilities and defensive vulnerabilities – “big stones, and plate glass windows,” said Lewis. “We’re back to mutually assured destruction.”

Others said that the military shouldn’t look any differently at hostile cyber actions than it would at physical attacks or efforts to undermine U.S. sovereignty.

“The U.S. posture has always been that ‘if you annoy us,’ we’ll do bad things,’ said Martin Libicki, a Senior Scientist at RAND. “We don’t need to be more specific than that.”

#### 8. No Retaliation — attribution failure prevents strikes.

Krepinivich 12 — Andrew Krepinivich, President of the Center for Strategic and Budgetary Assessments — a conservative budget thinktank, Ph.D. in International Studies from Harvard University, 2012 (“Cyber Warfare a ‘Nuclear Option’?,” *Center for Strategic and Budgetary Assessments,* August 24th, Accessible Online at <http://csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/>, Accessed On 6-30-2016)

As the discussion of attack attribution earlier in this report suggests, for at least the near term the source of a nuclear attack is far more likely to be identified than the source of a cyber attack. The difficulty in determining attribution of a cyber attack is a significant and perhaps enduring character of cyber warfare. This is due in part to the potential large number of actors that can execute cyber attacks, and to the relative ease by which cyber attackers can mask the origins of an attack. To date even substantial efforts to determine attribution of a sophisticated attack have not produced a “smoking gun” level of evidence, and have taken con- siderable time and resources to pursue. 237 This suggests that in the case of a cyber attack whose purpose is to inflict catastrophic destruction, the victim may have difficulty determining its source. To the extent this is the case, the victim will also want to avoid being deceived into engaging in a catalytic war by retaliating against the apparent source of an attack that was actually conducted by a third party. Moreover, cyber weapons could also be employed to trigger a catalytic nuclear war in other ways; for example, by feeding false information into a state’s early warning system to spoof operators into believing their country is under attack when in fact it is not. It seems unlikely that nuclear weapons could be employed to trigger a catalytic cyber war, at least given the current state of nuclear proliferation.

### Extend: “Cyber-cooperation Fails”

#### Cyber-cooperation fails — agreements are too vague and varying definitions of actions means that cooperation breaks apart. There’s no enforcement mechanism for Chinese compliance and data sharing, which ensures that scandals are inevitable. Denial of responsibility creates mutual distrust that undermines confidence building and norm formation — that’s Tiezzi.

#### U.S.-China cyber cooperation fails — no incentive.

Harold et al. 16 — Scott Warren Harold, Associate Director of the Center for Asia Pacific Policy at the RAND Corporation, Ph.D. in Political Science from Columbia University, M.A. in Political Science from Columbia University, B.A. in International Relations from Michigan State University, and Martin C. Libicki, Senior Management Scientist and Professor of Economics at the Pardee RAND Graduate School, Ph.D. in Economics from the University of California, Berkley, M.A. in Reigonal Planning from the University of California, Berkley, and Astrid Stuth Cevallos, Project Associate at the RAND Corporation, M.Phil. in International Relations from Oxford University, A.B. in East Asian Studies from Princeton University, 2016 (“Getting to Yes with China in Cyberspace,” *RAND Corporation*, May 2nd, Accessible Online at <http://www.rand.org/pubs/research_reports/RR1335.html>, Accessed On 06-30-2016, AS)

In conclusion, Chinese and U.S. views of cybersecurity overlap only on a few points, and even where they do, the two sides will find it difficult to make progress on such issues as avoiding targeting of critical infrastructure if the two sides struggle to maintain the progress hinted at in the September 2015 summit agreement on cyberspace. With respect to reaching a broad, meaningful, and lasting agreement on norms about legitimate targets in cyberspace, much work remains to be done, and it is unclear that such a result will indeed be possible. Perhaps the most promising area where we might see some prospect of negotiating a set of norms in the years ahead lies in avoiding targeting or carrying out espionage on critical infrastructure. This could be supported by efforts to create common standards of evidence, define how attribution is to be done, and prosecute those who commit such actions.

#### Cooperation Fails — stonewalling and denial.

Inserra 15 — David Inserra, Policy Analyst in Cybersecurity at the Heritage Foundation, 2015 (“4 Highlights From Obama’s Ridiculous Cyber Agreement With China,” *The Daily Signal,* September 29th, Accessible Online at<http://dailysignal.com/2015/09/29/4-highlights-from-obamas-ridiculous-cyber-agreement-with-china/>, Accessed On 07-01-2016)

1. [T]he United States and China…agree to cooperate…with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory.

Great, but think about the implications. The Chinese will request that the U.S. help it stop all sorts of dissident hackers and activists. The U.S. lives up to its agreements so it will dutifully help the Chinese even as oppressed individuals are jailed for cybercrimes, such as “jeopardizing Internet security” or accessing “illegal and harmful information,”—i.e., anything the Chinese Communist Party doesn’t like.

Then what stops the Chinese from stonewalling to protect their hackers? Will the Chinese help the U.S. investigate the five Chinese military officers that the U.S. charged with cybercrimes last year? Doubtful.

2. The United States and China agree that neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

The U.S. does not engage in economic espionage because it goes against U.S. principles of rule of law and property rights. However, while everyone knows that the Chinese engage in economic espionage, Beijing has always vigorously denied it.

Less than a week ago, Xi Jinping said, “The Chinese government does not engage in theft of commercial secrets in any form, nor does it encourage or support Chinese companies to engage in such practices in any way.”

He emphasized this point throughout his trip to the U.S. What, then, have the Chinese actually agreed to do? They have agreed to stop a behavior that they deny ever engaging in. That doesn’t bode well as an indicator of their future behavior.

### Extend: “US Cyber-Hypocrisy”

#### US led norm formation fails — revelations of NSA spying and economic espionage against Europe have destroyed US credibility on cybernorms. The US cannot convince others to follow the rules that they break. China in particular uses this as an excuse to avoid following and setting norms — that’s Gady.

#### Cyber-hypocrisy decks norm development.

Atlantic 12 — The Atlantic, Byline: Robert Wright, 2012 (“President Obama's Hypocrisy on Cyberattacks,” *The Atlantic,* June 3rd, Accessible Online at<http://www.theatlantic.com/international/archive/2012/06/president-obamas-hypocrisy-on-cyberattacks/258016/>, Accessed On 07-01-2016)

So even as Obama was issuing a clarion call for a global norm against the use of cyberweapons, he was seeing to it that America violated that norm in spectacular fashion. Or, as Jason Healey of the New Atlanticist puts it, "The arsonist wants to legislate better fire codes." (The hypocrisy was originally, but more tentatively, noted by Eric Martin of the Progressive Realist last year when the cyberspace manifesto was released and American involvement in the development of Stuxnet had been reported more conjecturally.)

Healy notes that hypocrisy isn't exactly a new thing in the affairs of nations. But, as he also notes, there are times when the exposure of hypocrisy is particularly costly. One is when you face the dawn of a new technological age and you're trying to establish rules of the road that will benefit countries like yours in particular. A reasonably effective global norm against cyberwarfare wasn't an impossible dream, but thanks to President Obama, it may be now.

According to Sanger, Obama "repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks." I guess he gets credit for having the concerns. He'd get more credit if he had shown the wisdom to act on them.

#### Stuxnet and Prism undermine norm setting.

Guardian 13 — The Guardian, Byline: Julian Borger, 2013 (“Obama faces hypocrisy charges at China summit after data mining revelations,” *The Guardian,* June 7th, Accessible Online at <https://www.theguardian.com/world/2013/jun/07/obama-hypocrisy-china-summit-surveillance>, Accessed On 07-01-2016)

President Xi does not need to prove equivalence, however. He just has to point to the contradictions between America's stated ideals and the way those ideals have been compromised in the pursuit of security. Obama has helped muddy the water for him.

Addressing the surveillance disclosures on Friday, Obama pointed out: "You can't have 100% security and also 100% privacy, and also zero inconvenience. We're going to have to make some choices as a society."

The question posed by this week's revelations is whether his administration has made the right choices on behalf of American society or whether the dream of near-perfect security has taken undue precedence over the way of life the state is supposed to be securing. Translated on the world stage – on which Obama must stand today – the question is whether the pursuit of overwhelming hard power has come too much at the expense of the softer variety.

One of the most relevant examples has been the cyber-attacks mounted on Iran, in which the US is widely and convincingly reported to have taken part, along with Israel. The Stuxnet worm slipped into Iranian uranium enrichment systems may have crashed hundreds of centrifuges, but three years later it is clear it did nothing to halt the steady progress of the Iranian nuclear programme. But it did generate a storm of controversy over the legality of the attack. That controversy is a burden on Obama today as he tries to convince Xi to accept strict new rules-of-the-road for cyber behaviour.

Similarly, the row over the US National Security Agency's collection of telephone data and the tapping into the computer systems of US internet providers under the Prism program hamstrings Washington when it tries to set global norms for internet freedom and privacy, just as the continued existence of the Guantánamo prison camp hampers the US government's efforts to set standards for basic human rights.

### Extend: “No Impact Uniqueness”

#### The total number of incidents between the US and China is rapidly decreasing. China is dismantling most of their cyberattack network. The impact didn’t occur during much higher frequencies of hacking, so it won’t occur now — that’s Gady.

#### Sanction threats reduced Chinese cyber-attacks by 90 percent — recent reports confirm

Uchill 16 — Joe Uchill, the first Mark Clayton Fellow in Cybersecurity, is a one-time applied mathematician, 2016 ("Obama administration confirms drop in Chinese cyber attacks," *The Hill*, June 28th, Available Online at http://thehill.com/policy/cybersecurity/285153-obama-administration-confirms-drop-in-chinese-cyber-attacks, Accessed 06-29-2016, AS)

A top Obama administration official on Tuesday confirmed private sector reports that Chinese hacking had plummeted in the past year.

“It seems like there has been a change in activity,” U.S. Assistant Attorney General John Carlin told a crowd at a Center for Strategic and International Studies event. “There is a debate as to how long lasting it might be, but there has been a change”

Last week, the security firm FireEye reported that attacks from China-based groups may have dropped as much as 90 percent over the last two years.

Carlin also predicted that hacking sanctions against other countries – which were outlined in an executive order in April of last year but have never be enforced – would begin being a more commonplace occurrence. The order gives the secretary of the Treasury, "in consultation with the Attorney General and the Secretary of State," the ability to impose sanctions.

“If we’re going to have the world where the norm is enforced, once we start using it, it has to become a regular part of business,” he said.

### Extend: “Norms Fail”

#### Norms Fail — there is no guarantee that countries will comply with norms because of lack of attribution capacity and enforcement mechanism. Entrenched interests in global militaries and governments are strongly against cyber-disarmament. Countries will either openly refuse to comply or will go underground, making attacks more untraceable — that’s Stevens.

#### Norms with China Fail — differing ideals make them meaningless.

Inserra 15 — David Inserra, Policy Analyst in Cybersecurity at the Heritage Foundation, 2015 (“4 Highlights From Obama’s Ridiculous Cyber Agreement With China,” *The Daily Signal,* September 29th, Accessible Online at<http://dailysignal.com/2015/09/29/4-highlights-from-obamas-ridiculous-cyber-agreement-with-china/>, Accessed On 07-01-2016)

3. Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community.

This point underscores how little the U.S. understands with whom it is negotiating. The Chinese have a dramatically different view of cyberspace and warfare. For them, their cyber operations, ranging from the economic to the more traditional government espionage, are just parts of their larger warfare strategy during peacetime. On a domestic level, the U.S. believes the Internet is a tool that enriches commerce and freedom, while the Chinese government fears the Internet for the same reasons.

Norm development (agreeing that certain types of behavior are wrong) may constrain actors who all agree to core principles, but when coming from such radically different places, norm development is meaningless.

#### Cybernorm development doesn’t prevent attacks.

Segal 11 — Adam Segal, Ira A. Lipman Chair in Emerging Technologies and National Security and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, Ph.D. in Government from Cornell University, M.A. in International Relations from Tufts University, B.A. in Government from Cornell University, 2011 (“Cyberspace Governance: The Next Step,” *Council on Foreign Relations,* March, Accessible Online at <http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397>, Accessed On 07-01-2016)

International cooperation is necessary, but some fundamental characteristics of cyberspace make traditional arms control agreements unlikely. The technologies used in most attacks are commercial and widely available. Attacks can be masked and routed across several networks, obscuring whether they are the work of independently operating "patriotic hackers," criminal groups, an official security agency, bored teenagers, or some combination of all four. This problem of attribution undermines verification; signatories to any agreement would have little confidence they could identify violators.

Moreover, there is no consensus about what constitutes a cyberattack. The United States talks primarily about defending critical infrastructure like the power grid or financial systems; China, Russia, and others worry about these vulnerabilities but also see the free flow of information as a threat to domestic stability. As a result, in any negotiations, Beijing and Moscow are likely to demand that the United States limit its support for "digital activists" in return for China and Russia controlling "patriotic hackers," a requirement Washington is unlikely to meet.

### Extend: “Long Timeframe”

#### Timeframe for norm development is massive — it takes years of harsh political horse-trading to come to a consensus. It took decades to come to a consensus on nuclear weapon use, and cyberspace is no different — that’s Nye.

#### Norm development takes decades and treaties are impossible.

FCW 15 — FCW, Byline: Zach Noble, 2015 (“Can the U.S. push the world to accept cyber norms?,” *FCW,* December 21st, Accessible Online at <https://fcw.com/articles/2015/12/21/noble-cyber-norms.aspx>, Accessed On 06-30-2016, MA)

Americans have been pushing for cyber norms at the U.N. since President Barack Obama's 2011 International Strategy for Cyberspace, but the going has been painfully slow. A 2013 report from the U.N.'s Group of Governmental Experts presented a substantial -- but voluntary -- list of norms, including applying international law to the cyber realm and holding states responsible for attacks originating inside their own borders. And in September, Obama and Chinese President Xi Jinping announced a common understanding on cyber issues.

"This is a no-kidding presidential priority," said Chris Painter, the State Department's coordinator for cyber issues, at a Dec. 18 panel discussion hosted by the Center for Strategic and International Studies. "This really is something the president feels strongly about." Norms that prohibit nations from cyberattacking one another's critical infrastructure and promote cooperation in cyber investigations, as the Group of Governmental Experts agreed to this summer, are exactly what the world needs, Painter argued, even if they are not binding. “The more countries you have, even if [the standards are] voluntary, it really creates what the standard of behavior is," he added. "It really allows countries to rally around those, and if people are outside, it will act against them in the long term."

But real global agreement on cyber norms is a long way off. "It's going to take years and maybe decades" until the world comes to a more holistic cyber agreement, said Catherine Lotrionte, director of Georgetown University's Institute for Law, Science and Global Security. "We're not going to have a universal treaty signed on all activities in cyberspace." And even within the talks, "the United States may not be the best country to drive some of those discussions," said Ian Wallace, senior fellow and co-director of New America's Cybersecurity Initiative. Small nations, such as early e-government-adopter Estonia or the Netherlands, might help lead the way in U.N. discussion groups, panelists said.

### Extend: “Bias to Overhype”

#### Their evidence is biased to overhype the threat — no one reads a headline unless it says something sensational. Their authors all use statistics created by the military and government who have an incentive to overestimate the threat for funding reasons. China’s threat is relatively small, and not unique — that’s Gady.

#### Media overestimates the threat and ignores evidence.

Schneier 13 — Bruce Schneier, Chief Technology Officer at Resilient, an IBM Company, Fellow at Harvard’s Berkman Center, Board Member of the Electronic Frontier Foundation, 2013 (“Nationalism on the Internet,” *Crypto-Gram*, March 15th, Accessible Online at <https://www.schneier.com/crypto-gram/archives/2013/0315.html>, Accessed On 07-01-2016)

Our nationalist worries have recently been fueled by a media frenzy surrounding attacks from China. These attacks aren't new -- cyber-security experts have been writing about them for at least a decade, and the popular media reported about similar attacks in 2009 and again in 2010 -- and the current allegations aren't even very different than what came before. This isn't to say that the Chinese attacks aren't serious. The country's espionage campaign is sophisticated, and ongoing. And because they're in the news, people are understandably worried about them.

But it's not just China. International espionage works in both directions, and I'm sure we are giving just as good as we're getting. China is certainly worried about the U.S. Cyber Command's recent announcement that it was expanding from 900 people to almost 5,000, and the NSA's massive new data center in Utah. The U.S. even admits that it can spy on non-U.S. citizens freely.

The fact is that governments and militaries have discovered the Internet; everyone is spying on everyone else, and countries are ratcheting up offensive actions against other countries.

At the same time, many nations are demanding more control over the Internet within their own borders. They reserve the right to spy and censor, and to limit the ability of others to do the same. This idea is now being called the "cyber sovereignty movement," and gained traction at the International Telecommunications Union meeting last December in Dubai. One analyst called that meeting the "Internet Yalta," where the Internet split between liberal-democratic and authoritarian countries. I don't think he's exaggerating.

Not that this is new, either. Remember 2010, when the governments of the UAE, Saudi Arabia, and India demanded that RIM give them the ability to spy on BlackBerry PDAs within their borders? Or last year, when Syria used the Internet to surveil its dissidents? Information technology is a surprisingly powerful tool for oppression: not just surveillance, but censorship and propaganda as well. And countries are getting better at using that tool.

But remember: none of this is cyberwar. It's all espionage, something that's been going on between countries ever since countries were invented. What moves public opinion is less the facts and more the rhetoric, and the rhetoric of war is what we're hearing.

The result of all this saber-rattling is a severe loss of trust, not just amongst nation-states but between people and nation-states. We know we're nothing more than pawns in this game, and we figure we'll be better off sticking with our own country.

Unfortunately, both the reality and the rhetoric play right into the hands of the military and corporate interests that are behind the cyberwar arms race in the first place. There is an enormous amount of power at stake here: not only power within governments and militaries, but power and profit amongst the corporations that supply the tools and infrastructure for cyber-attack and cyber-defense. The more we believe we are "at war" and believe the jingoistic rhetoric, the more willing we are to give up our privacy, freedoms, and control over how the Internet is run.

### Extend: “No Risk of Cyberwar”

#### Chances of Cyberwar with China are Remote — Diplomatic initiatives build trust, and prevent conflict via diplomatic horse trading. Deterrence checks any risk of escalation and prevents devastating attacks because of fear of starting conflict — that’s Roberts.

#### Cyberwar is overhyped — deterrence checks and no impact.

Vijayan 10 — Jaikumar Vaijayan, Editor of Tech Beacon, citing Marcus Ranum, Faculty Member at the Institute for Applied Network Security, and James Lewis, Senior Fellow at the Center for Strategic and International Studies, 2010 (“Senators ramp up cyberwar rhetoric,” *Computer World,* April 2nd, Accessible Online at <http://www.computerworld.com/article/2516720/security0/senators-ramp-up-cyberwar-rhetoric.html>, Accessed On 06-30-2016)

\*The bill mentioned is the Snowe-Rockefeller Bill.

The proposed bill has its share of supporters, but the cyberwar rhetoric being used to justify the need for such measures is viewed skeptically by growing numbers of IT security professionals. Warnings about cyberwar, especially in the wake of the China-based attacks against Google and more than 30 other high-tech companies, is unnecessary overhyping of what's going on, some experts say.

One of them is noted security researcher Marcus Ranum, chief security officer at Tenable Network Security Inc. In an opinion piece in U.S. News and World Report earlier this week, Ranum warned that the cyberwar rhetoric is scarier than actual war.

"Suddenly, the steady drumbeat of computer/network security has been pushed to center stage, and now our government is talking about 'cyberwar' and pointing a finger at China," Ranum wrote. "Unless you've been asleep for a decade, you ought to be worried when our government starts using the rhetoric of warfare -- especially vocabulary like 'preemptive' and 'deterrence.'"

Ranum today said that concerns about catastrophic economic losses and social havoc stemming from a cyberwar are misplaced.

"When some cyberwar pundit starts talking hellfire and damnation, you need to ask them whether their scenario is going to have the physical and psychological impact of a New Orleans flood or a 9/11," Ranum said in e-mailed comments to Computerworld. The types of disruptions that some people claim cyberwar will cause, such as large-scale power blackouts, are unlikely to result in the kind of mayhem that is being assumed, he said. Many "experience power failures sometimes lasting days -- because of winter weather -- and we don't dissolve into chaos," he said.

Ranum's views are similar to those of a growing number of other experts. James Lewis, who headed a team that developed a set of cybersecurity recommendations for President Obama, recently wrote about the issue in a blog. The nation is not in the middle of a cyberwar, Lewis stressed.

Drawing a comparison to traditional warfare, he noted that it's unlikely that a country would preemptively launch a missile strike against critical infrastructure in the U.S., because it would fear massive retaliation. The same holds true for cyberwar, said Lewis, who is a senior fellow and program director at the Center for Strategic and International Studies. "Foreign leaders will not lightly begin a war with the United States," he said. "And the risk of cyberwar is too high for frivolous or spontaneous engagement."

#### Risk of cyberconflict is overhyped — small attacks don’t justify conflict.

Lewis 14 — James Lewis, Senior Vice President and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, 2014 (“Explained: Why a U.S.-China "Cold War" in Cyberspace Is Not Happening,” *The National Interest,* November 12th, Accessible Online at <http://nationalinterest.org/blog/the-buzz/explained-why-us-china-cold-war-cyberspace-not-happening-11655>, Accessed On 06-30-2016, MA)

Describing cyber activities by the US and China as a new Cold War in cyberspace is hyperbolic and inaccurate. The relationship between the US and China and the international environment for this relationship are very different from the Cold War, when relations and contacts with the Soviet Union were extremely limited and there was no economic interdependence or interconnection. There have been none of the threats, ideological challenges or proxy conflicts that characterized the Cold War.

The US has sought to avoid a military focus in its cybersecurity efforts. It has cast China’s cyber espionage as a commercial matter (Treasury Secretary Lew has told China’s President that cyberattacks are ‘a very serious threat to our economic interests’). For example, the US indictments of People’s Liberation Army officers for cyber espionage focused intentionally on trade and economic crimes to avoid any implication that this was a military contest.

China has never used “force” (defined as acts of violence) against the US in cyberspace; it will use cyberattack against US military forces in any clash, but espionage isn’t war—if it were grounds for war, the US would find itself at war with many countries. Both China and the US have implicitly avoided truly damaging attacks or military confrontation in cyberspace, each restricting its activities to espionage. Espionage isn’t a crime under international law, and it’s not in the US interest to make it so. Dealing with China’s cyber espionage requires a sustained effort to construct norms and persuade China to observe them, to create consequences for Chinese actions, and to improve cyber defences in the interim.

### Extend: “No Retaliation”

#### No Retaliation — countries aren’t irrational. They have a high standard for military action against other states. Absent convincing evidence against another country, escalation is unlikely. Nuclear escalation carries an extremely heavy weight — Krepinivich.

#### Cyberwar won’t escalate – they remain regionalized and restrained.

Gartzke and Lindsay 15 — Erik Gartzke, Associate professor of Political Science at the University of California, San Diego, and Jon Lindsay, Senior Fellow at the University of California Institute on Global Conflict and Cooperation, 2015 (“Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace,” *Security Studies,* June 22nd, <http://www.researchgate.net/publication/279069843_Weaving_Tangled_Webs_Offense_Defense_and_Deception_in_Cyberspace>, Accessed On 06-30-2016)

Indeed, the US Department of Defense gets attacked ten million times a day; a US university receives a hundred thousand Chinese attacks per day; and one firm measures three thousand distributed denial of service (DDoS) attacks per day worldwide.23 In reality, however, most of these so-called attacks are just routine probes by automated networks of compromised computers (botnets) run by profit-seeking criminals or spy bureaucracies—a far cry from terrorism or military assault. The most alarming scenarios of a “digital Pearl Harbor” or “cyber 9/11” have yet to materialize despite decades of warning.

The Stuxnet worm caused limited and temporary disruption of Iran’s nuclear program in the late 2000s, the only known historical case of infrastructure damage via deliberate cyber attack, but this operation seems to reveal more about the strategic limitations of cyber war than its potency. The cyber revolution should presumably provide rivals with potent new tools of influence, yet actual cyber disputes from 2001 to 2011 remain restrained and regionalized, not disruptive and global. Computer espionage and nuisance cybercrime thrive, to be sure, but they are neither as prevalent nor as costly as they might be, leading skeptics to describe US losses as “a rounding error” in a fifteen trillion dollar economy.26 It is possible in principle that the same tools used for computer-network exploitation may one day be leveraged for more destructive strikes. Yet even if the nontrivial operational challenges of cyber war can be overcome, proponents of the cyber-revolution thesis have yet to articulate convincing strategic motives for why a state or non-state actor might actually use cyber capabilities effectively.27

### They Say: “Competitiveness Impact”

#### No competitiveness or economy impact — the impact is minimal.

Austin 15 — Greg Austin, Professorial Fellow at the East-West Institute, Professor at the Australian Center for Cybersecurity, 2015 (“Why the China-US Cyber Agreement May Prove Destructive,” *The Diplomat,* October 7th, Accessible Online at <http://thediplomat.com/2015/10/why-the-china-us-cyber-agreement-may-prove-destructive/>, Accessed On 06-28-2016, MA)

First, the United States overestimates the negative impact of China’s cyber espionage on U.S. competitiveness. Take for example the case of Westinghouse, the giant U.S. corporation named as a victim in the indictments brought against five People’s Liberation Army (PLA) personnel in May 2014 for commercial espionage. Westinghouse was almost certainly the victim of cyber espionage and its trade secrets were undoubtedly handed to a Chinese competitor.

But within two months of the indictment, Westinghouse raised its estimates of likely new contracts in China to US$20 billion. Its competitiveness does not appear to have been impacted negatively in the short to medium term. And Westinghouse was already in a long term technology transfer relationship with China that had seen it hand over some 75,000 technical documents as well as engaging in joint nuclear construction projects in China.

Second, the U.S. position rests on its assertion that there is a workable and enforceable distinction between the national security purposes of economic cyber espionage (which Washington defends and conducts) and the commercial purposes of cyber espionage (which Washington says it opposes). In effect, the United States is implying very clearly that the espionage against Westinghouse had no national security implications at all. Such a claim is not sustainable. There may be few companies in the United States where the blurring between military and civil purposes is more profound. Westinghouse is a major supplier of military nuclear reactors to the U.S. Navy. For this reason, Westinghouse and the nuclear technology sector appear therefore to have been poor choices for action by the United States as part of a diplomatic strategy to counter China’s cyber espionage for being commercial in character.

## Elections DA

### Link — Hard on Cybersecurity

#### Voters prefer hardline cyber security policies towards China

Diaz 15 ― Brittni Diaz, writer for Enterprise Risk Management, 2015. (“Cyber Security’s Role in the 2016 Election”, *EM Risk*, Novemeber 4th, 2015, Available Online at: <http://info.emrisk.com/blog/bid/78464/Cyber-Security-s-Role-in-the-2016-Election> Accessed 6-30-16)

The topic of cybersecurity has been thrust into the headlines of many big stories as of late. Major hacks like the Target, Sony Pictures, App Store and Ashley Madison breaches have all made the public aware of how destructive cyber attacks can be. So it is no surprise that cyber security will be an important topic during the 2016 presidential election.

As technology progresses, governmental entities are spending more and more time working to protect data by preventing cyber attacks. What does this mean for the presidency? China is already a big concern and has been mentioned in recent presidential debates. Donald Trump and Hillary Clinton have both publicly blamed China for data breaches.

The solution to Chinese attacks lie in stronger cyber security for governmental agencies and entities that store secure and sensitive information. Candidates will likely call on the need to improve national cyber security, and many may also take a more offensive approach. While there has not been much discussion of retaliatory measures, polls show Americans are in favor of taking action against countries or groups behind cyber attacks. So many sensitive industries are vulnerable to cyber attacks, like the healthcare, airline and automotive industries. As more attacks occur, candidates will have to take a definitive stance on the cyber security issue.

#### Cybersecurity is key to the older voters

Nasr 15 ― Amir Nasr, journalist for the Morning Consult, 2015. (“For 2016 Hopefuls, Chasing Older Vote Might Mean Beefing Up Cyber Defense”, *Morning Consult*, September 28th, 2015, Available Online at: <https://morningconsult.com/2015/09/28/for-2016-hopefuls-chasing-older-vote-might-mean-beefing-up-cyber-defense/> Accessed 6-30-16)

As presidential candidates look to attract older voters, they might want to follow in the footsteps of former Florida Gov. Jeb Bush (R) or former Maryland Gov. Martin O’Malley (D) and beef up their cybersecurity platforms. O’Malley and Bush are the only presidential candidates who have put forward specific plans of how to address cybersecurity.

A new poll from Morning Consult shows that large majority of older voters want to hear more from their candidates on the topic of cybersecurity, much more than those in younger groups.

Sixty-nine percent of registered voters aged 65 or older called for increased cybersecurity dialogue from 2016 candidates. Every other age group polled had a far lower rate of agreement that candidates should talk more about the issue. Voters between the ages of 55 and 64 were at 49 percent. Those between 45 and 54 were at 36 percent. The other age groups hovered just under half.

Overall, 49 percent of registered voters think 2016 candidates should be talking about cybersecurity more, compared to 27 percent who believe they are talking about the issue the right amount and 7 percent who think candidates should be talking less about it.

#### Older voters are key to the election

Easley 6/24 ― Jason Easley, journalist for Politicus USA, 2016. (“One Chart Shows The Biggest Lesson That Democrats Need To Learn From Brexit Vote”, *Politicus USA*, June 24th, 2016, Available Online at: <http://www.politicususa.com/2016/06/24/chart-shows-biggest-lesson-democrats-learn-brexit-vote.html> Accessed 6-30-16)

An election with lower turnout dominated by older voters looks eerily similar to how Republicans win midterm elections in the US:

[Graph Omitted]

The lesson for Democrats from Brexit is that younger voters have to turn out to vote. If the electorate is dominated by an older demographic, Donald Trump odds of winning will increase. Younger voters did not want to leave the EU, but since they didn’t show up at the polls in large enough numbers, they are now going to be harmed by a potentially disastrous result that was determined by the older generations.

The principle behind both Brexit and US elections is the same. When younger voters don’t show up in large enough numbers, conservatives win. Donald Trump may be a self-destructive fool, but if the electorate is small enough, old enough, and white enough, he could win the White House in November.

#### Cyber security issues is key to the election

Robinson 15 ― Rick Robinson, journalist for Security Intelligence, 2015. (“Cybersecurity a Major Topic in 2016 Presidential Election”, *Security Intelligence*, November 24th, 2015, Available Online at: <https://securityintelligence.com/cybersecurity-a-major-topic-in-2016-presidential-election/> Accessed 6-30-16)

Don’t look now, but cybersecurity is lurking as a major issue in the developing U.S. presidential election cycle. The stage has been set by developments in the seven years since the last election with no incumbent on the ballot.

In 2008, no one had heard of the Target or Sony hacks, the Stuxnet worm or Dyre malware. Hardly anyone cared about Facebook’s privacy policy. Most people thought of cybercriminals as bright but maladjusted teenagers, and Internet crime meant emails from fake Nigerian widows.

In short, the cybersecurity era has come of age. But its full political implications are only now beginning to emerge, and we don’t yet know the level of importance cybersecurity will take in the upcoming presidential election.

Professionals Look for an Understanding

A survey of cybersecurity professionals by Tripwire found that 68 percent of them preferred to vote for a presidential candidate with a strong cybersecurity policy. But as one expert put it, there is “a big difference between a candidate who has a cybersecurity policy and a candidate who has an understanding of cybersecurity.”

Cybersecurity professionals hardly compose a strong voting bloc, and presidential campaigns will target them not for votes but rather to win support from cybersecurity thought leaders. Their views could help shape public perceptions of a complex issue that most people cannot expect to understand on their own.

Just to complicate things, the cybersecurity issue does not always go by that name. In this day and age, privacy as an issue refers chiefly to online and data privacy, which means to say cybersecurity as viewed through a privacy lens.

An Issue that Takes Many Forms

How safe are people’s computers and mobile devices from snooping? How safe is the personal data such as credit card numbers they have entrusted to companies and other organizations? What about their data stored in the cloud? Are people even aware that whatever they put on their devices is being stored in the cloud? These issues are all about cybersecurity.

Public concern about cybersecurity is also subject to cross-cutting concerns. Privacy protection wins strong support on both the right and left, but with differences in focus: Conservatives are more likely to worry about foreign threats, liberals about prying by business, and both sides may be suspicious of government snooping and cybersecurity policies.

Enterprise security, which is a major concern of cybersecurity professionals, may not strongly engage the electorate in and of itself — people are more likely to scoff at corporate victims than to feel sorry for them. But enterprise breaches also expose consumers, giving voters a stake in corporate cybersecurity, as well.

Given the complexities of the issue and the many forms it takes, cybersecurity by that name may not directly emerge as a campaign battleground issue. But whether as concern about terrorism, government intrusion or consumer financial protection, cybersecurity issues in one form or another are likely to be prominent in the 2016 presidential election.

### Security

#### Cyber impacts are constructed ― products of an impending cyber apocalypse is created by the military-industrial complex

Hansen and Nissenbaum 9 ― Lene Hansen, Associate Professor in the Department of Political Science at the University of Copenhagen, Ph.D. in Political Science from University of Copenhagen, M.A. in Political Science from University of Copenhagen, B.A. in Political Science from University of Copenhagen; Helen Nissenbaum, Professor in the Department of Media, Culture and Communication at New York University, Ph.D. in Philosophy from Stanford University, M.A. in Social Sciences in Education from Stanford University, B.A. in Mathematics and Philosophy from University of the Witwatersrand, 2009. (“Digital Disaster, Cyber Security, and the Copenhagen School”, *International Studies Quarterly*, 2009, Available Online at: <https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>, Accessed 06-30-16, p.1163-1164)

The first concept, hypersecuritization, has been introduced by Buzan (2004:172) to describe an expansion of securitization beyond a ‘‘normal’’ level of threats and [end page 1163] dangers by defining ‘‘a tendency both to exaggerate threats and to resort to excessive countermeasures.’’ This definition has an objectivist ring to it in that to identify ‘‘exaggerated’’ threats implies that there are ‘‘real’’ threats that are not exaggerated. Moreover, the question of whether a securitization is seen as ‘‘exaggerating’’ concerns the degree to which it is successful (unsuccessful securitizations are seen as ‘‘exaggerating’’) and is not part of the grammatical specificities of sectors. Thus we suggest to drop the ‘‘exaggerated’’ from the definition of hypersecuritization and to apply it to the cyber sector to identify the striking manner in which cyber security discourse hinges on multi-dimensional cyber disaster scenarios that pack a long list of severe threats into a monumental cascading sequence and the fact that neither of these scenarios has so far taken place.

All securitizations do of course have an element of the hypothetical in that they constitute threats that must be countered, and thus mobilize an ‘‘if-then’’ logic, but what distinguishes hypersecuritizations from ‘‘mere’’ securitization is their instantaneity and inter-locking effects (Denning 1999:xiii). This combination draws critically from the securitization of the network (Deibert 2002), yet the power of hypersecuritization stems not only from a securitization of the network itself, but from how a damaged network would cause societal, financial, and military break-down hence bringing in all other referent objects and sectors.

Securitizations always mobilize the specter of the future to some extent, but most nevertheless articulate the past as a legitimating reference that underscores the gravity of the situation. Looking to the Cold War, the logic of nuclear deterrence relied upon projections of a nuclear exchange that had not taken place, yet there were the devastations of Hiroshima and Nagasaki to be used as a yardstick for what nuclear war would imply. Cyber securitizations on the other hand have no similar history of founding incidents to base themselves on but try to conjure historical analogies such as ‘‘electronic Pearl Harbors’’ (Bendrath 2003:50).7 The combination of cascading disasters and the absence of a prior incident of that magnitude creates a crucial ambiguity within cyber security discourse. The extreme reliance on the future and the enormity of the threats claimed at stake makes the discourse susceptible to charges of ‘‘exaggeration,’’ yet the scale of the potential catastrophe simultaneously raises the stakes attached to ignoring the warnings.8 Turning the absence of prior incidences in the opposite direction, the difficulty of saying that it could not happen also creates a powerful space for the projection of the (im)possible.

## Capitalism K

### Link — Cybersecurity

#### Cyber security prioritizes market structures while ignoring structural vulnerabilities created by neoliberalism

Cavelty 14 ― Myriam Cavelty, senior lecturer for security studies at the Center for Security Studies, Senior Lecturer for Security Politics at ETH Zurich, Visiting Fellow at the Watson Institute for International Studies at Brown University, Ph.D. from University of Zurich, M.A. in History from University of Zurich, 2014. (“Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities”, *Science and Engineering Ethics*, September 2014, Volume 20, Issue 3, Available Online at: <http://link.springer.com/article/10.1007%2Fs11948-014-9551-y>, pg. 704-707, Accessed 06-30-16)

A general basic issue for cyber-security is that the information infrastructure that we use every day for data-transfer was never built with security in mind: vulnerabilities abound. One of the reasons for the continued existence and constant new creation of these vulnerabilities is that security is constantly ‘‘underproduced’’ in a market dominated by the so-called network effect, under which the benefits of a product increase when the number of users increases, and the ‘‘winner takes it all’’. Quasi-monopolies and time pressures lead to a focus on fast delivery in commercial software development. Quality criteria, like security, play only a minor role (Anderson and Moore 2006). Another reason is that the most powerful actors providing the most important information services today have an interest in keeping them insecure: Big Data is considered the key IT trend of the future, and companies want to use the masses of data that we produce every day to tailor their marketing strategies through personalized advertising and prediction of future consumer behaviour (Morozov 2013). Therefore, there is no interest in encrypted (and therefore secure) information exchange. On top of this, the intelligence agencies of this world have the same interest in data that can be easily grabbed (Bo¨hme 2005).

The human in this threat discourse is the weakest link that creates vulnerabilities i.e. through ‘‘faulty’’ software development, or the human is a hapless victim that is exploited by i.e. the actions of cyber-criminals. Through the economic damage that is produced that way, the threat is linked back to the economic security and welfare and often back to national security (Dunn Cavelty and Suter 2012). However, humans are also the prime threat in the archetype/stereotype of the ‘‘hacker’’, individuals with technical superpowers, able to easily pose a sever threat to powerful actors with very limited resources (at least in theory) (Conway 2008; Barnard-Wills and Ashenden 2012).

Vulnerable Critical Objects

The selection of a ‘‘referent object’’ of security is closely interrelated with how the threat is represented. As mentioned, some objects—commonly called infrastructures—and the functions they perform are regarded as ‘critical’ by the authorities (in the sense of ‘vital’, ‘crucial’, ‘essential’) because their prolonged unavailability harbours the potential for major crisis, both political and social (Burgess 2007). In the mid-1990s, the issue of cyber-security was persuasively interlinked with this topic of ‘‘critical infrastructures’’ and their necessary protection and in the process made into a salient national security issue (PCCIP 1997). Because critical infrastructures combine symbolic and instrumental values, attacking them becomes integral to a modern logic of destruction (Coward 2009: 408f.) that seeks maximum impact.

One classical goal of (national) security is to throw a ‘‘protective or preservative measure […] around a valued subject or object’’ (Dillon and Lobo-Guerrero 2008: 276). Before this security can unfold, the valued subject/object needs to be identified and also localized in space. In cyber-security linked to critical infrastructure protection, the identification and designation of the protection-worthy is performed following the well-established steps of (technical) risk analysis techniques, which contains both an act of ‘‘naming’’ and an act of prioritizing. At the beginning of such an analysis stands the identification of the assets (including services) that are critical: Criticality is seen as a measure of the consequences associated with the loss or degradation of a particular asset or object. Therefore, criticality needs a reference point: it can only exist in relation to something (pre-)defined as important and normal/desirable (Brunner et al. 2010).

Cyber-security linked to critical infrastructures creates and is implemented in a special type of security environment. Whereas the traditional logic of national security suggests unilateral government action and policy, the policies of cyber-security are inevitably blurred by liberalization, domestic considerations and other policy imperatives (Coaffee and Murakami Wood 2006). The management of infrastructure is in general not (or no longer) the prerogative of government; instead it is based on the logic of the market. While it remains the essential task of a government to provide the security of society, it has simultaneously become impossible for any government to achieve this by itself. What is at stake is not the body of the state or its borders, ‘‘but the conjoined body of public and private-sector networks’’ (Der Derian and Finkelstein 2008: 102). Therefore, the private sector becomes instrumental in not only helping with the act of ‘‘identification’’ of critical objects, but also more directly in assuring the health of networks and the services provided by them.

Whereas the methodology employed to identify critical assets is very similar in both the public and private sector, the commonalities end when it comes to the protection goals. From the public sector’s perspective, criticality is linked to the loss of one or more broad national functions. That set of functions—or protection principles—has expanded over time, beginning with national defense and economic security, to include public health and safety, and then national morale (Kristensen 2008). Through definition of these national functions along the lines of general well- being of a nation and its citizens, the link between critical infrastructure protection and national security is forged. For the state, the goal of protection is the collective well-being represented as a way of liberal life (Anderson 2010)—but, by implication, also the continued function of the state. The relationship between state and infrastructure emerges as an alternative to the image of Abraham Bosse’s Leviathan on the frontispiece of Hobbes famous book: Instead of being made up of its citizens, the state is regarded as consisting of the things inside its territory that make life there ‘good’; assets that are not directly identified with its citizens, but material assets that give substance (and significance) to the state through being its foundation (Dunn Cavelty and Kristensen 2008).

For the private sector, the reference point varies depending on the business model; in the abstract, however, it is their functioning, or ‘business continuity’, that is the ultimate protection goal. The reference object for companies, therefore, is themselves. Crucial for the continued performance and effectiveness of many of today’s companies that operate as traders of information/knowledge with the help of information/knowledge networks, is protection against loss of information and routine preservation of knowledge. These techniques sever the human mind/body as ‘‘’incubator’ of this knowledge’’ from the knowledge itself (Der Derian and Finkelstein 2008: 102), which is given autonomous value over that which becomes replaceable as a result of these practices. In this view, humans become reduced to nodes in the network, needed to ensure the wealth and health of the networks, but not their own health.

National Security versus Human Security in Cyberspace

In cyber-security as currently understood and practised, human beings are seen as victims, as weakest link in the system, as direct threat—but not (or only very indirectly) as beneficiaries of the type of security that states (and companies) want. On the one hand, the neglect of the human element is a direct consequence of a focus on technical systems as targets and technology-based countermeasures in cyber-security. On the other hand, the lack of consideration for ‘‘the human’’ in this field also seems to be an effect of the issue that human security scholarship has already tackled decades ago: that too much focus on the state and national security tends to crowd out consideration for the individual citizen, with often detrimental effects for security overall (cf. Burgess and Owen 2004). I look at both aspects and their consequences for security below and then turn to the clash between this type of security and human security.

Technical Systems, Political Consequences

A focus on technical objects is not a bad thing per-se. In fact, the type of security that emerges directly from the wish to ensure cyber-security is one that seemingly dodges problematic issues normally associated with security, at least in the first instance. Ultimately, we are looking at the practice of protecting inanimate things; the regulation of machines and their performance. Computers, servers, and the computer-powered infrastructures are non-human objects, which are someone’s legitimate property and have a certain (usually undisputed) value for societies. Cyber-security measures thus imagined have little to no bearing on citizens’ lives directly. Most importantly, there are no concerns about freedom/security trade-offs, and no civil liberty issues (Buzan et al. 1998). This security does not depend upon the invocation of a state of emergency, but is ‘clean’ and ultimately, ‘good’, since everybody seems to benefit from an interruption-free performance of vital systems.

However, this view is inevitably problematized, because these machines cannot be isolated from human life. The image of modern complex critical infrastructures is one in which it becomes futile to try and separate the human from the technological. Technology is not simply a tool that makes life livable: rather, technologies become constitutive of novel forms of ‘a complex subjectivity’, which is characterized by an inseparable ensemble of material and human elements (Coward 2009: 414). Therefore, even if technologies may appear to regulate objectively and apolitically, there is always a connection to a place, to a space, to a space of protection, to values, to life. An even closer look at the seemingly apolitical management of a technical issue with technical means reveals a deeply political nature, because the selection of referent objects as described above always entails a larger argument about protection: Endangered entities are judged to have legitimate claims to protection (while others do not). In other words, this type of security will only provide relief to a valued referent object—not necessarily ‘‘the citizen’’ or humans more generally.

In cyber-security, as argued above, economic imperatives like profit maximization are decisive. It is not a given, then, that cyber-security is a truly public good, understood as security for all. Quite the opposite: the type of security that emerges mainly benefits a few and already powerful entities and has no or even negative effects for the rest. The type of referent object to be protected and by implication, the type of life to be saved, is represented by the uninterrupted flow of information linked to the accumulation of capital and economic growth (Swyngedouw 2007), which in turn is linked to national security. This is at the heart of the cyber-security dilemma, in which the dominant form of security is making large parts of the population arguably less secure. Various security needs are not aligned; and while they do not always have to be, more awareness of the clash between them is needed.

## Cybersecurity Sanctions CP

### Notes

The counterplan solves the cybersecurity advantage by implementing sanctions on Chinese cybercriminals.

### 1NC — Cyber Sanctions CP

#### [THE FIRST/NEXT OFF-CASE POSITION IS THE CYBER SANCTIONS COUNTERPLAN]

#### Text: The United States federal government should implement sanctions on Chinese cyber criminals, companies, and foreign intelligence operatives that benefit from cybercrime.

#### Sanctions change Chinese cyber actions — indictments prove.

WaPo 15 — Washington Post, Major US Newspaper, citing, James Lewis, Cyberpolicy Expert at the Center for Strategic and International Studies, and Rob Knake, Whitney Shepardson Senior Fellow at the Council on Foreign Relations, 2015 (“China shifts commercial hacking away from military to civilian agency,” Byline Ellen Nakashima*,* November 30th, Accessible Online at <https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html>, Accessed 06-29-2016, MA)

Then in May 2014, the Justice Department, following a months-long FBI investigation, announced the indictments of five PLA officers on economic espionage charges. One of the accused was a hacker profiled in the Mandiant report — a moon-faced, bespectacled officer named Wang Dong, also known by the online moniker Ugly Gorilla.

“The indictments had an amazing effect in China, more than we could have hoped for,” said James A. Lewis, a cyber-policy expert at the Center for Strategic and International Studies. “The Chinese hated them. They complained about them every time there was a meeting. They said there couldn’t be any progress [in cyber-talks, which the Chinese pulled out of] until the indictments were withdrawn and we promised not to do them again.”

In the following months, the Chinese military quietly began dismantling its economic espionage apparatus, officials said. PLA leaders, with Xi’s approval, reviewed the military’s cyber-activities. They cracked down on moonlighters within the PLA who were hacking on the side to sell information to companies, and they attempted to halt collection of data that was not central to the national security mission.

What the change in PLA activity shows is that “China is not this implacable, immovable object,” said Rob Knake, a senior fellow at the Council on Foreign Relations and a former White House cyber-official. “We can in fact alter the behavior of at least portions of the Chinese government.”

In April, Obama signed an executive order establishing the power to impose economic sanctions on individuals and entities that take part in or benefit from illicit cyber-activities such as commercial espionage.

“If the indictments had the effect of getting the PLA to scale down, then sanctions likely will have a wider effect on other Chinese state-sponsored groups,” Knake said.

### 2NC/1NR — Overview

#### The affirmative grants China false legitimacy — sanctions are vital.

Inserra 15 — David Inserra, Policy Analyst in Cybersecurity at the Heritage Foundation, 2015 (“4 Highlights From Obama’s Ridiculous Cyber Agreement With China,” *The Daily Signal,* September 29th, Accessible Online at<http://dailysignal.com/2015/09/29/4-highlights-from-obamas-ridiculous-cyber-agreement-with-china/>, Accessed On 07-01-2016)

This point doubles down on the flawed ideas expressed earlier in the document. But it also betrays a key assumption present throughout the document: the Chinese are victims and partners in the fight against cyber criminals.

Regrettably, this is a huge step back to the mindset the Obama administration held years ago. China is not a partner and it is not a victim—it is the perpetrator.

By granting China moral equivalence with the U.S., the Obama administration has sacrificed the moral high ground, giving the Chinese exactly what they want—legitimacy. The U.S. government has now all but adopted the Chinese position and language on cyber policy, surrendering to Chinese demands in exchange for a nice sounding press release. What is worse, this agreement will probably stop the U.S. from implementing any of the cyber sanctions waiting in the wings against China.

This agreement will do nothing to keep the U.S. safe in cyberspace, but gives China the moral and political legitimacy they want on this issue and will likely keep important cyber sanctions at bay.

Of course we could just trust everything the Chinese say. And if that’s the case, I’ve got a bridge to sell you in China.

#### Sanctions deter cybercrime and provoke Chinese shifts.

Bertrand and Kelley 15 — Natasha Bertrand, Geopolitics Editor at Business Insider, M.A. in Government from the London School of Economics, and Michael Kelley, Senior News Editor at Business Insider, M.A. in Journalism from Northwestern University, 2015 (“The Obama administration just opened a new 'weaponization of finance' front,” *Business Insider,* April 1st, Accessible Online at <http://www.businessinsider.com/us-sanctions-against-cyber-hackers-2015-4>, Accessed 06-29-2016, MA)

Subjecting cyber criminals, companies that benefit from commercial espionage, and even foreign intelligence operatives to tough financial sanctions could have a "momentous" effect in deterring the growing number of cyberattacks seen daily on US networks, said Dmitri Alperovitch, chief technology officer of Crowdstrike, a cybersecurity firm.

"Today, the White House is making yet another huge leap forward in the effort to raise the cost to our cyber adversaries and establish a more effective deterrent framework to punish actors engaged in serious intentional destructive or disruptive attacks," Alperovitch wrote in a blog posted on the company’s website

The program could prompt a strong reaction from China. Cybersecurity has been a significant irritant in US-China ties, with US investigators saying hackers backed by the Chinese government have been behind attacks on US companies, and China rejecting the charges.

#### Even the threat of sanctions is enough to deter cyberattacks

Gady, 1AC Author, 16 — Franz-Stefan Gady is an Associate Editor with The Diplomat.His interests include civil-military relations, revolution in military affairs, and cyber diplomacy. He also is a Senior Fellow with the EastWest Institute. Franz-Stefan has reported from a wide range of countries and conflict zones including Afghanistan, Iraq, and Pakistan. His writing and photos have appeared in The International New York Times, BBC News, Foreign Affairs Magazine, Foreign Policy Magazine, The National Interest, Vice News, The Middle East Eye, The Christian Science Monitor, Profil, Der Standard, and Die Presse among other publications. Franz-Stefan also has provided expert commentary for Asia News Weekly, Al Jazeera America, Channel News Asia, CCTV, PBS, Voice of America, Radio France, SCPR, and ORF among others. Janurary 28th, 2016. Key to U.S.-China Cyber Diplomacy Accessed 06-29-16 BYK

First, while it is true that attribution, i.e. tracing back a cyber attack to its originator, remains difficult, it is not impossible. Both the U.S. government and the private sector have repeatedly called out Chinese hackers in so-called “naming and shaming” campaigns. This tactic consists of either leaking classified intelligence to the press or publishing cyberattack reports by U.S. cyber security firms (which over the years became a clever marketing ploy for those companies). While “naming and shaming” sustained a severe setback with the Snowden revelations, we will certainly witness a number of such cyberattack disclosures in 2016. However, the shock value—and as a consequence its potential negative impact on the Sino-U.S. bilateral relationship—will be less severe than in 2014 and 2015, given that, after the recent Office of Personal Management data breach and the Snowden disclosures, the threshold for disclosures with the potential to severely undermine the Sino-U.S. bilateral relationship has substantially risen. At the same time, “naming and shaming” will at least contain both sides from going overboard when it comes to cyber espionage activities and aggressive network intrusions.

Second, sanctions, while an imperfect tool, appear to have caught the attention of the Chinese leadership in 2015 and will likely play a role in Sino-U.S. relations in 2016 as well. On April 1, 2015, U.S. President Barack Obama signed Executive Order 13694, which argues that “the increasing prevalence and severity of malicious cyber enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.”

As a consequence, the Obama White House threatened China with economic sanctions and individual Chinese citizens with travel restrictions should Beijing not rein in its hacker community. One indication that this worked has been the arrest of a number of Chinese hackers prior to the September 2015 state visit by Chinese President Xi Jinping, although there is considerable debate among experts whether there is a genuine connection between the two events. However, the threat of economic sanctions will have significantly higher impact on the senior Chinese leadership in 2016, primarily due to China’s deteriorating economic situation, but also due to the international humiliation the country would suffer from being the first nation subject to economic sanctions for cyber-attacks.